UNITED STATES DISTRICT COURT 5
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

UNITED STATES OF AMERICA	§	
	§	**Criminal No. 24-CR-00298**
V.	§	
	§	
EITHAN HAIM	§	

DEFENDANT'S REPLY IN SUPPORT OF MOTION TO DISMISS AND MOTION TO STRIKE

Although the government opposes dismissal, its implicit concessions require that result. The government takes two extraordinary positions. First, it abandons the Privacy Rule—which is the core of HIPAA—without a fight because it cannot defend the Rule's enforceability. Second, to compensate, the government expands the remainder of the HIPAA criminal provision so much that it too becomes unconstitutional. In doing all this, the U.S. Attorney's Office scuttles the authority of another executive department and opposes the position taken by the solicitor general before the Supreme Court. The Court must reject this lawless enterprise and dismiss this case. No further amendment could save the superseding indictment.

ARGUMENT

I. The Government's Implicit Concessions

The government fails to defend even a sliver of its authority to enforce the Privacy Rule with criminal effect or to explain what "this part" means in 42 U.S.C. § 1320d-6. That effectively eviscerates HIPAA. It is unprecedented. The

government simply does not try HIPAA criminal cases without relying on the HIPAA regulations to form the core of the criminal allegations. Every HIPAA case the government cites relied *only* on that basis for a criminal violation, not the "without authorization" language.[1] When people, or even lawyers, speak of HIPAA, they generally mean the Privacy Rule. And, as discussed below, the invalidity of the Privacy Rule means that the government's theory of "without authorization" is unviable too. When the government calls the defense's interpretation "problematic and strange, rendering 42 U.S.C. § 1320d-6 nearly toothless," it actually refers to the effects of the government's abandonment of its authority under the regulations necessary to give content to the statute.

The government does not address the effect of its concessions, but the superseding indictment cannot go forward. A core part of the argument in Dr. Haim's motion to dismiss is that the government cannot give meaningful content to "this part" in 42 U.S.C. § 1320d-6 for this case. The government asserts that "the elements comprising the offense are clear, and there is no need to resort to the HIPAA privacy regulations to understand it." But it then reworks the statutory language to be even more muddled without answering the central question.[2] The government never says

[1] Although the *Zhou* case uses the term "without authorization" in the opinion, that appears to derive from not having patient authorization, which is one way under the Privacy Rule to obtain records. The conduct occurred well before Congress added "without authorization."

[2] The government mashes several parts of the statute together to read: "A defendant is guilty if he (a) knowingly and in violation of this part, (b) obtained individually identifiable health information

what "this part" is or what falls within that term except "without authorization." Yet the superseding indictment still has the following clause: "and for a reason other than those permitted by Title 42, United States Code, Chapter 7, Subchapter XL [sic], Part C (provisions of HIPAA)." It would be bad enough for a nonexistent statutory reference (to Subchapter XL) in the superseding indictment to go back to the jury. But the entire clause must go. By disavowing the Privacy Rule, there are no longer any "reasons" the government can say are "permitted" or not by "this part." This language materially broadens the potential criminal conduct and could confuse the jury but has no content, so the Court must strike it. *See United States v. Trice*, 823 F.2d 80, 89 n.8 (5th Cir. 1987); *United States v. Bullock*, 451 F.2d 884, 888 (5th Cir. 1971). That said, fixing the obsolete clause would not save the superseding indictment because the problems it demonstrates pervade the entire theory of the government's case.

II. The Government's Theory of Without Authorization Is Untenable

The government proposes leaving the meaning of "without authorization" to the jury as a pure question of fact, with no further legal elaboration. Opp. at 6–10. Beyond causing innumerable problems, discussed below, that approach was squarely rejected by the Supreme Court. *See Van Buren v. United States*, 593 U.S.

['IIHI'] relating to an individual maintained by a covered entity without authorization." Opp. at 5. This makes it appear that the information must be obtained "in violation of this part" separately from being obtained "without authorization"—which of course requires use of the Privacy Rule.

374, 388–89 (2021). The government tries to create a gulf between the phrase "without authorization" in the CFAA and in HIPAA, but none exists. True, "without authorization" modifies different verbs, but it functions the same way in each. The operative language in the CFAA is "accesses a computer without authorization . . . and thereby obtains," 18 U.S.C. § 1030(a)(2), while in HIPAA it is "obtained . . . such information without authorization," 42 U.S.C. § 1320d–6(a). So while an "on/off, access-based definition for authorization" used in the CFAA does not literally work, Opp. at 7, an on/off, obtain-based definition for authorization does. It is the very same "gates-up-or-down inquiry" for authorization.

The question in HIPAA is whether the person was categorically authorized to obtain IIHI by the covered entity that maintains it, just as for the CFAA the question is whether the person was categorically authorized to access the computer by the entity maintaining the computer. Indeed, even the government does not treat the practical difference between obtaining IIHI and accessing IIHI as significant—the government uses the two concepts interchangeably and even expects Dr. Haim to defend himself by showing that the hospital "authorized him to access patient records" for the patients at issue. Opp. at 8, 10. Moreover, the similarity should surprise no one. The purpose of HIPAA according to Section 261 of that statute is "encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of

certain health information." Accordingly, the inquiry will be determined by whether the entity granted a user technological authentication such as login credentials—just as it is for the CFAA post-*Van Buren*. *See* Orin S. Kerr, *Focusing the CFAA in* Van Buren, 2021 Sup. Ct. Rev. 155, 170–80 (2021).

The alternative that the government functionally proposes, that the entity maintaining the IIHI sets rules on accessing IIHI any violation of which becomes a crime, was also squarely rejected by the Supreme Court in *Van Buren*. *See* 593 U.S. at 392–96. Indeed, the government's refusal to cut "for a reason other than those permitted by . . . provisions of HIPAA" from the superseding indictment yet its contradictory reliance solely on "without authorization" make doubly clear that it believes it can punish for accessing (or obtaining) IIHI for the wrong "reason"—for any reason contrary to hospital policy. *Van Buren* reversed the conviction for "accessing the law enforcement database for an 'inappropriate *reason*.'" 593 U.S. at 381 (emphasis added). And the facts of that case are closely analogous here: an employee (here, a resident) accessed (here, obtained) personal information in an official database that he was not permitted to access for the particular reason he had. *Id.* at 380.

Even under the superseding indictment, there is no question that the hospital provided Dr. Haim the ability to obtain *any* of the IIHI he is alleged to have obtained or that the hospital's policy did not categorically bar him from doing so—instead,

the appropriateness was to be determined *after* he received "authorization" (the gates were up) under rules dependent on later-existing conditions. Because he was granted authority to obtain *any* of the relevant IIHI under some conditions, obtaining them without those conditions was still not "without authorization." In other words, the "only question is whether [Dr. Haim] could use the system to retrieve [patient] information. Both sides agree that he could. [Dr. Haim] accordingly did not 'excee[d] authorized access,'" much less obtain that information "without authorization." *Van Buren*, 593 U.S. at 396.

The explanation of "without authorization" in Dr. Haim's motion to dismiss simply makes more sense, too. The motion posits that the world of those subject to HIPAA criminal liability is divided into two groups: those who are "covered entities" and everyone else. Covered entities, including health care providers who transmit "health information in electronic form," 42 U.S.C. § 1320d–1(a)(3), would necessarily have "authorization" to obtain and disclose IIHI because those tasks are definitional to being a covered entity. Everyone else—those who do not electronically transmit health information—generally does not have such "authorization." As Congress originally wrote the statute in 1996, HIPAA covered only the first group. When OLC made clear that HIPAA did not cover the second, Congress added the "without authorization" clause to do so. That addition was never meant to pull in or apply to covered entities. The Privacy Rule governing covered

entities works on fine-grained, use-based rules (that depend on the purpose or reason for handling IIHI), Mot. at 20, while the authorization inquiry is a simple yes-or-no inquiry agnostic to those concerns, *see Van Buren*, 593 U.S. at 390–91. This scheme would have worked to capture all relevant conduct between the two groups where privacy is concerned—except that Congress failed to make the Privacy Rule enforceable. This left a hole in which the charged conduct here falls.

That Congress failed to follow through with making the Privacy Rule enforceable may be unfortunate, but it is not inexplicable. Privacy is a controversial issue requiring nuanced rules. And although Congress hoped that it could solve the problem later after receiving recommendations from the Department of Health and Human Services, Section 264 of HIPAA made clear that Congress realized it might not. While Congress authorized HHS to then create privacy regulations, its choice not to give criminal effect to those novel, controversial rules in advance is also commendable (and constitutionally required). Yet as in most cases where one Congress leaves important work to a later one, those later Congresses have also not taken responsibility for addressing the issue comprehensively. Instead, they have only chosen a few pieces of the Privacy Rule to instantiate in the criminal code and left the remainder for yet future Congresses to address.

The government attempts to fix the hole left by Congress by expanding "without authorization" to try to cover it up. It cannot legally do so. That approach

does not accord with the text or legislative history.[3] And it renders the Privacy Rule, were that rule to be effective (which the government still maintains it is without argument), overlapping with and duplicative of "without authorization." This renders the government's interpretation not only wrong, but unconstitutional.

III. The Government's Approach Leads to Monstrous and Unconstitutional Absurdities

As with many attempts by the executive to act where Congress shrunk back, its arrogation of power creates a myriad of problems. The government's approach, beyond usurping Congress's role, also leads to true absurdities that demonstrate how gravely the government errs. This approach imports all the problems identified in decades of litigation over the CFAA. But its interpretation goes further, breaking new ground in the scope of its lawlessness.

To start, the overlap between the Privacy Rule and "without authorization" under the government's approach creates intolerable conflicts. By means of that overlap, the government seeks to sneak the Privacy Rule into a criminal case through the back door. In refusing to defend the validity of the Privacy Rule, the government flatly disclaims any need for it: "the elements comprising the offense are clear, and there is no need to resort to the HIPAA privacy regulations to understand it." Opp.

[3] Indeed, the House Ways and Means Committee Report that the government and the Ninth Circuit (*United States v. Zhou*, 678 F.3d 1110 (9th Cir. 2012)) cited concerns the original HIPAA statute. Opp. at 8. *Zhou* dealt with conduct before the statute was revised. Although Congress thought privacy was "paramount," *id.*, that does not mean Congress ever figured out how to address the issue.

at 5. Yet a mere four pages later, when it comes time to defend its position against the many problems created by allowing each hospital to set its own rules, the government "resort[s] to HIPAA privacy regulations to understand it." The government states, without a modicum of conscientiousness:

> [T]he defendant also ignores the fact that all covered entities are governed by the same HIPAA privacy regulations. Hospital policies regarding who can use or disclose patient records and under what circumstances are informed by HIPAA's privacy regulations, ensuring a significant degree of uniformity across institutions.

Opp. at 9. As the defense already demonstrated uncontested, covered entities are not meaningfully governed by HIPAA privacy regulations, and certainly not criminally. So the government is really saying the following: even though the Privacy Rule is not criminally enforceable on its own, because hospitals *think* that they are governed by the Privacy Rule and use it to set their policies, it *becomes* criminally enforceable without the government having to defend it. This double-dealing alone should make clear the absurdity of the government's position. But it gets much worse.

The overlap and backdoor effect of the Privacy Rule creates a conundrum. If the overlap is complete and the Privacy Rule duplicative (and especially if it has criminal effect), then Congress has created a great deal of surplusage in adding "without authorization." But the situation is worse if "without authorization" is under- or over-inclusive. Partial overlap simply presents the odd scenario where some, but not all, privacy violations are doubly criminalized. The greater concern

comes if a hospital can prohibit conduct—here, obtaining IIHI under certain circumstances—that the Privacy Rule allows. The motion to dismiss previewed this concern, Mot. at 15, and the government all but conceded that this could occur, Opp. at 9–10. It is no small matter. The Privacy Rule's use- and purpose-based permissions include broad reasons for obtaining IIHI,[4] such as for "treatment, payment, or health care operations," 45 C.F.R. § 164.502(a)(1)(ii), and also a large number of nuanced, specific exceptions. Some, such as using patient information to de-identify that information or using it to "prevent or lessen a serious and imminent threat to the health or safety of a person," 45 C.F.R. §§ 164.502(d); 164.512(j), are relevant to Dr. Haim's defense. Yet the government's position allows the hospital to prohibit these at will. That is the necessary consequence of making authorization a fact-based inquiry dependent on the particularities of the hospital's policies.[5]

The implications are staggering. If a hospital can prohibit disclosures to law enforcement (*see* 45 C.F.R. § 164.512), it can, for instance, criminalize reports of its

[4] The superseding indictment alleges that the hospital "only authorized [Dr. Haim] to review patient records of patients under his care." Dkt. No. 76 ¶ 7. While the vagueness of these terms presents another problem, if that was truly the hospital's policy, then it contravened the Privacy Rule because it is substantially and materially more restrictive. At the same time, any restrictions that solely mirror the Privacy Rule cannot overcome the obtain/use mismatch. *See* Mot. at 19–20.

[5] While the government may assert that a defendant can use the Privacy Rule as a shield, that already concedes that the government's "without authorization" inquiry has serious problems because huge swathes of its facial effect must be carved out as inconsistent with other law. And the solution provides cold comfort. At the very least, it again makes the "without authorization" inquiry merely duplicative of the Privacy Rule, with the change that now the Privacy Rule provides only an affirmative defense, to be demonstrated after indictment and at trial.

own criminality. And if the government offices involved are ideologically aligned, prosecutorial discretion will not save a whistleblower from being punished.

Yet that fact pattern does not exhaust the potential absurdities. Indeed, the more mundane and insignificant the rule, the more egregious for receiving a criminal penalty for its violation. Consider a rule that prohibits doctors from obtaining patient information except through their own EMR accounts. Even though a doctor might have every right to a patient's information under the Privacy Rule because he is treating that patient, it becomes a crime for the assisting nurse to show the doctor that patient's chart. Or consider a rule requiring that doctors using remote access have a safe workspace at home before logging on. Does a malfunctioning smoke detector render a doctor a criminal, too?

The government's approach also renders the statutory prohibition unconstitutional in several ways, all noted in the context of the CFAA but worse here. Handing authority to draft rules with criminal penalties over to hospitals and other health care entities—private actors who are by no means legislatures or even expert draftsmen—leads to many constitutional infirmities. Several courts, and the Supreme Court, noted the related problems of vagueness and notice with a policy-based version of the authorization terms in the CFAA. *See Van Buren*, 593 U.S. at 394; Note, *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 Harv. L. Rev. 751, 753–61 (2013). Due process requires

providing "fair notice of the conduct [the law] punishes" and prohibits criminal liability "so standardless that it invites arbitrary enforcement." *Johnson v. United States*, 576 U.S. 591, 595 (2015). There is no way to tell from the HIPAA statute what rule will determine the criminality of the conduct, no way to ensure that the private policies are clear, and no bulwark against arbitrary enforcement. *See United States v. Nosal*, 676 F.3d 854, 860–62 (9th Cir. 2012) (en banc).

Any policy-based limitations have a related, fatal flaw. As discussed in the motion to dismiss (and as with the CFAA), Mot. at 20, the HIPAA criminal provision does not govern use. But purpose-based limits on accessing or obtaining information are typically designed with an eye toward misuse and "can be expressed as either access or use restrictions." *Van Buren*, 593 U.S. at 396. So criminality will turn on whether the hospital frames the policy as withholding authorization to obtain records for certain uses or simply prohibiting those uses. Yet any policy, purpose-based or not, creates the same arbitrariness. *See* Kerr, *supra*, at 179 (exploring gradations in various access policies). "An interpretation that stakes so much on a fine distinction controlled by the drafting practices of private parties is hard to sell as the most plausible." *Van Buren*, 593 U.S. at 396.

More concretely, as the examples above demonstrate, having liability hinge on private policies makes liability turn on factual minutiae. A strictly factual inquiry has potentially unlimited complexity, including the serious questions noted in the

motion to dismiss: Who has actual or apparent authority to explicitly or implicitly amend hospital polices? Can senior doctors who run the programs do so by practice? What if a policy exists informally and multiple administrators have different understandings? What effect do trainings have, and can they provide evidence of the meaning of or interpret otherwise ambiguous hospital provisions? How do the policies apply to non-employee physicians, such as residents? None of these are mere hypotheticals; they are likely to be implicated at a trial in this case.

Although the government scoffs at these factual difficulties, retorting that juries "routinely consider complex factual issues" such as contractual provisions, the courts have not been so flippant. Indeed, the en banc Ninth Circuit specifically noted that turning workplaces relationships "governed by tort and contract law" into "ones policed by the criminal law" creates constitutional problems. *Nosal*, 676 F.3d at 860. "Significant notice problems arise if we allow criminal liability to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read." *Id.* While the law tolerates civil liability turning on an ex-post determination of complex contractual provisions that are ambiguous ex ante, for criminal law the liability must be clear up front.

Yet whatever notice problem was present with broader interpretations of authorization in the CFAA, the situation is worse here for HIPAA. The government asserts that notice is irrelevant because no *mens rea* concerning a policy violation is

required. Opp. at 8–9. In other words, the government believes that HIPAA creates a worse-than-strict-liability crime. Even strict liability crimes must make clear *what* is prohibited. The law must provide *some* notice. *See Staples v. United States*, 511 U.S. 600, 612–13 (1994). Yet here, according to the government, the hospital can change its authorization policies on a whim, not provide any notice, and render any doctor a criminal. Offenses without *mens rea* requirements are "disfavored," *id.* at 606, and the Fifth Circuit has assiduously avoided interpreting crimes as strict liability unless absolutely required by Congress, *see United States v. Garrett*, 984 F.2d 1402, 1409 (5th Cir. 1993) (collecting cases). If the notice that would guarantee *mens rea* cannot bend, then the scope of the conduct covered must, and "without authorization" must be construed narrowly.

Additionally, allowing the hospital to set conditions under which doctors are authorized to obtain IIHI, on pain of federal criminal law for any violation, represents an unconstitutional delegation of authority to a private actor. This problem was noted in the discussion over the meaning of authorized access in the CFAA. *See generally* Note, *supra*. The very same concerns motivated the only court to squarely consider the issue to reject the approach of criminalizing violations of terms of service and similar policies. *See Sandvig v. Barr*, 451 F. Supp. 3d 73, 88 (D.D.C. 2020). Granting criminal sanction to the rules a website sets "risks turning each website into its own criminal jurisdiction and each webmaster into his own

legislature." *Id.* The same result follows here with hospitals setting rules on using their electronic medical records systems to obtain patient information.

These constitutional defects in the government's approach are severe enough to invalidate its interpretation if accepted. But they need not be to require that the narrower interpretation of "without authorization" be chosen. All that is required is that the government's position present "serious constitutional doubts." *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 516 (2009). And it does so in spades. There is also no question that the narrower interpretation is one of two "fair alternatives," *United States v. Davis*, 588 U.S. 445, 465 (2019). It was already the heavy favorite given *Van Buren*. So if it is even necessary to reach the issue, the Court should apply the doctrine of constitutional avoidance to narrow the meaning of "without authorization"—which also accords with the rule of lenity.[6] *Id.*

CONCLUSION

The government's attempt to save its superseding indictment only creates new, more egregious problems. Its positions are inconsistent with the text, purpose, and legislative history of HIPAA—and with the Department's own interpretation of the same terms elsewhere. The Court should do what the government refuses and end this prosecution, which has no basis in law.

[6] The Supreme Court has been particularly careful to adopt the narrower versions of ambiguous provisions that Congress tacks onto the end of more detailed schemes. *See, e.g.*, *Fischer v. United States*, 144 S. Ct. 2176, 2187 (2024).

Dated: November 13, 2024

Respectfully submitted,

/s/ Marcella Burke
Marcella C. Burke
TX State Bar 24080734
SDTX No. 1692341
Burke Law Group, PLLC
1000 Main St., Suite 2300
Houston, TX 77002
Tel: 832.987.2214
Fax: 832.793.0045
marcella@burkegroup.law

Ryan Patrick
Attorney-in-Charge
TX State Bar 24049274
SDTX No. 3006419
Haynes and Boone LLP
1221 McKinney Street, Suite 4000
Houston, Texas 77010
Tel: 713.547.2000
Fax: 713.547.2600
ryan.patrick@haynesboone.com

Jeffrey A. Hall
VA State Bar 82175
SDTX No. 3885025
Burke Law Group, PLLC
2001 L. Street N.W., Suite 500
Washington, D.C. 20036
Tel: 832.968.7564
Fax: 832.793.0045
jeff@burkegroup.law

Mark D. Lytle
DC Bar 1765392
SDTX No. 3884197
Nixon Peabody LLP
799 9th Street NW, Suite 500
Washington, D.C. 20001
Tel: 202.585.8435
Fax: 202.585.8080
mlytle@nixonpeabody.com

ATTORNEYS FOR DEFENDANT EITHAN DAVID HAIM

CERTIFICATE OF SERVICE

The undersigned attorney hereby certifies that a true and correct copy of the above and foregoing document has been filed and served on November 13, 2024 using the CM/ECF system, which will send notification of such filing to all counsel of record.

/s/ *Marcella C. Burke*
Marcella C. Burke